



# AOS 17.09.01.00 Release Notes

Release Notes

Release Date: Sept. 24, 2010

Notes Revision: Sept. 24, 2010

## Introduction

NetVanta Series products support application image updates via the ADTRAN OS Web GUI, TFTP, X-Modem, and FTP. A detailed firmware upgrade guide with step-by-step instructions is available at:

<http://kb.adtran.com/article.asp?article=1630&p=2>.

Prior to upgrading firmware, please ensure that your unit meets the minimum Boot ROM requirements, listed under "Supported Platforms."

## Supported Platforms

	<u>Standard Feature Pack</u>	<u>Enhanced Feature Pack</u>	<u>Minimum Boot ROM****</u>
NetVanta 1234/1238	9700594-2A170901.biz	N/A	17.03.02.SB
NetVanta 1534	9700590-2A170901.biz	N/A	17.03.01.00
NetVanta 1534 2 <sup>nd</sup> Gen.	9702590-2A170901.biz	N/A	17.08.01.00
NetVanta 1534P 2 <sup>nd</sup> Gen.	9702590-2A170901.biz	N/A	17.09.01.00
NetVanta 1544/1544F	9700544-2A170901.biz	N/A	17.05.01.00
NetVanta 1544 2 <sup>nd</sup> Gen.	9702544-2A170901.biz	N/A	17.08.01.00
NetVanta 1544P 2 <sup>nd</sup> Gen.	9702544-2A170901.biz	N/A	17.09.01.00
NetVanta 1335	N/A	9950515-2A170901.biz	15.01.00
NetVanta 3120	N/A	9700600-2A170901.biz	14.04.00
NetVanta 3130	N/A	9700610-2A170901.biz	14.04.00
NetVanta 3200/3205 (3 <sup>rd</sup> Gen.)*	9200860-2A170901.biz	9950860-2A170901.biz	17.02.01.00
NetVanta 3305	9200880-2A170901.biz	9950880-2A170901.biz	04.02.00
NetVanta 3430	9200820-2A170901.biz	9950820-2A170901.biz	13.03.SB
NetVanta 3430 2 <sup>nd</sup> Gen.	9202820-2A170901.biz	9952820-2A170901.biz	17.05.01.00
NetVanta 3448	9200821-2A170901.biz	9950821-2A170901.biz	13.03.SB
NetVanta 3450	9200823-2A170901.biz	9950823-2A170901.biz	17.06.01.00
NetVanta 3458	9200824-2A170901.biz	9950824-2A170901.biz	17.06.01.00
NetVanta 4305***	9200890-2A170901.biz	9950890-2A170901.biz	08.01.00
NetVanta 4430	9700630-2A170901.biz	9950630-2A170901.biz	17.04.01.00
NetVanta 5305	9200990-1A170901.biz	9950990-1A170901.biz	11.03.00

\*1<sup>st</sup> generation NetVanta 3200/3205 routers (part numbers beginning '1200') and 2<sup>nd</sup> generation NetVanta 3200/3205 routers (part numbers beginning '1202') cannot run this version of AOS.

\*\*1<sup>st</sup> generation NetVanta 3305 (Part number 1200880L1) cannot run this version of AOS.

\*\*\*1<sup>st</sup> generation NetVanta 4305 (Part number 1200890L1) cannot run this version of AOS.

\*\*\*\*To confirm the version of Boot ROM, telnet or console to the unit and issue the **show version** command. The Boot ROM version will be listed as **Boot ROM version XX.XX.XX**. If you require a Boot ROM upgrade, please contact ADTRAN Technical Support (support@adtran.com or 888-423-8726) for assistance.

New Features	Overview
<b>Proxy Users Template</b>	<p>This AOS feature allows for traffic from users (endpoints or IP PBXs) that are behind an AOS device and are not recognized by the SIP proxy to be routed. This is useful for those devices that do not register to a softswitch and IP PBXs that do not register one user for all phones.</p> <p><i>Supported Platforms</i>    <b>NetVanta 1335, NetVanta 3120, NetVanta 3130, NetVanta 3200, NetVanta 3205, NetVanta 3305, NetVanta 3430, NetVanta 3448, NetVanta 3450, NetVanta 3458, NetVanta 4305, NetVanta 4430, NetVanta 5305</b></p>

Enhancements	Overview
<b>Dial Backup Support on 2<sup>nd</sup> Generation Dual T1 NIM</b>	<p>The 2<sup>nd</sup> generation dual T1 NIM now provides support for the V.90 analog modem DIMs. The 2<sup>nd</sup> generation dual T1 NIM provides two T1/FT1 interfaces that have added the capability of being clocked independently of one another.</p> <p><i>Supported Platforms</i>    <b>NetVanta 1335, NetVanta 3200/3205, NetVanta 3305, NetVanta 3430/3448, NetVanta 3450/3458, NetVanta 4305, NetVanta 4430</b></p>
<b>VLAN-Aware Port Security</b>	<p>This AOS feature allows port security to be configured on VLAN trunked switchports. This is most commonly used to provide port security in applications where there is both voice and data traffic.</p> <p><i>Supported Platforms</i>    <b>NetVanta 1234, NetVanta 1238, NetVanta 1335, NetVanta 1534 (1<sup>st</sup> and 2<sup>nd</sup> Gen) &amp; NetVanta 1544 (1<sup>st</sup> and 2<sup>nd</sup> Gen), NetVanta 3448, NetVanta 3458</b></p>
<b>VRRP Support for NetVanta 3305</b>	<p>The Virtual Router Redundancy Protocol was introduced in AOS in revision 16.1 but is now also available on the NetVanta 3305.</p> <p><i>Supported Platforms</i>    <b>NetVanta 3305</b></p>
<b>SNMP Sub-Indexing</b>	<p>SNMP results will now present each sub-interface as a separately indexed interface instead of being presented as the parent interface.</p> <p><i>Supported Platforms</i>    <b>NetVanta 1335, NetVanta 3200, NetVanta 3205, NetVanta 3305, NetVanta 3430, NetVanta 3448, NetVanta 3450, NetVanta 3458, NetVanta 4305, NetVanta 4430, NetVanta 5305</b></p>

## Errata

*These are issues that were discovered during internal testing, but were unresolved at the time of release.*

- Disabling 802.1q encapsulation on an Ethernet interface may not restore the port-authentication command.
  - Workaround: Rebooting the AOS device will allow for the port-authentication command to be restored.
- When stacking is configured, the stacking VLAN may not come up after the switchport stack mode is modified on a stack member.
  - Workaround: Do not modify the switchport stack mode.
- The NetVanta 3120/3130 may fail to answer incoming calls on the DBU interface.
  - Workaround: No known workaround.
- Port-Auth re-authentication cannot be forced on an individual switchport.
  - Workaround: Use the global 'port-auth re-authentication' command.
- On the 2<sup>nd</sup> Gen NetVanta 1534 and NetVanta 1544 the 'show ip interface' command may make reference to an Ethernet interface where none exists.
  - Workaround: No known workaround. This is a display issue.
- Traffic may not pass over a link that is configured to bridge over Frame-Relay.
  - Workaround: Configure PPP instead of Frame-Relay.
- A passphrase for a wireless network that is configured using the Wireless wizard may not persist when the wizard is completed.
  - Workaround: Configure the passphrase manually through the GUI or CLI. Keys can be used instead of a passphrase.
- If Desktop Auditing and Network Forensics are enabled and a broadcast storm occurs, the AOS device may reboot.
  - Workaround: Disable desktop auditing and network forensics or enable storm control to prevent a broadcast storm.
- The 3G and WWAN NIM may stop responding resulting in the error message on the demand interface that states, "No data call resource."
  - Workaround: Reboot the AOS device.
- When using MAC-based port-authentication, the EAP-request will not initiate after a link bounce unless both the authenticator and supplicant see the link bounce.
  - Workaround: Do not place another switch or hub between the supplicant and the authenticator.
- Deleting an ATM interface in AOS may cause the device to reboot.
  - Workaround: Shutdown ATM interface and then delete it.
- The System page in the Web GUI will display a 503 error if there is a PPP interface present and the Ethernet interface was chosen as the public interface in the Setup Wizard.
  - Workaround: Manually configure the Ethernet interface through the CLI or GUI.
- Spanning tree commands may not appear under the HDLC interface in the CLI.
  - Workaround: No known workaround.
- Configuring bridging may create a new spanning-tree instance instead of using the STP 0 instance.
  - Workaround: No known workaround..
- Counters for hardware ACLs with multiple permit and deny statements may not increment correctly.
  - Workaround: No known workaround.
- GVRP may not properly remove VLANs after a viable VLAN path has been removed.
  - Workaround: No known workaround.
- On the NetVanta 2<sup>nd</sup> Gen 1534P, the Web GUI may return an error stating, "Error getting menu: ReferenceError: set Collapse is not defined" when attempting to load the menu.
  - Workaround: Refresh the webpage.
- On the NetVanta 2<sup>nd</sup> Gen 1534, tearing down port-security in the CLI may not be reflected in the web GUI.
  - Workaround: No known workaround.
- Shutting down a dialup interface while it is being used with an analog modem may cause the AOS device to reboot.
  - Workaround: Do not shut down the dialup interface or disconnect a call.
- The NetVanta 4430 may exhibit CRC errors when passing data over an analog modem.

- Workaround: No known workaround.
- Configuring the demand interface through the web GUI may erroneously set the MTU to 0.
  - Workaround: Configure the demand interface or manually set the MTU through the CLI.
- Under certain conditions, an AOS device which has 802.1x configured may allow an unauthorized supplicant, which is authenticating using an incorrect password, to pass traffic.
  - Workaround: Reboot the unit.
- Physically removing a DBU connection causes the CLI to continuously output the following error message, “Connect failed (No Resources Available). Retry in 10 seconds!”
  - Workaround: No known workaround. The command ‘no dial-backup’ will stop the error message from being outputted.
- On the NetVanta 3450 and 3458, the analog modem DIM may not be recognized by an AOS device on bootup.
  - Workaround: Reboot the router.
- Switchports on the NetVanta 1534 and 1544 may erroneously negotiate to 100 Mbps.
  - Workaround: Hardset the speed of the switchport.
- When configuring proxy template users, the CLI will output an error whenever a dash is used in ‘accept’ and ‘reject’ commands.
  - Workaround: Use commas with the ‘accept’ and ‘reject’ commands instead.
- The Security Audit on the NetVanta 1534PoE may not recognize that ‘service password encryption’ is enabled.
  - Workaround: No known workaround.
- On the NetVanta 2<sup>nd</sup> Gen 1544P, in the web GUI, clicking on the map name in the ACL configuration tab on the hardware ACL page takes you to the traffic selector page.
  - Workaround: Configure hardware ACLs using the CLI.
- The NetVanta 2<sup>nd</sup> Gen 1534P may not allow a user to clear a hardware ACL entry.
  - Workaround: Delete the hardware ACL.
- The stacking VLAN may not come up if switchport stack mode is first removed and then re-added on a stack member.
  - Workaround: Do not bounce the switchport stack mode on a stack member.
- The 2<sup>nd</sup> Gen NetVanta 1534 may not correctly apply SNMP settings when adding an SNMP server host, using SNMP version 3, and not specifying a username.
  - Workaround: No known workaround.
- The NetVanta 2<sup>nd</sup> Gen 1544 may show an SFP port in an up/up state even though the cable is unplugged.
  - Workaround: Manually shut down the port.
- The web GUI may not completely remove a wireless MAC ACL when deleted.
  - Workaround: Delete the wireless MAC ACL through the CLI.
- The Netvanta 2<sup>nd</sup> Gen 1534 may output “speed duplex mismatch” errors when there are no speed or duplex mismatches.
  - Workaround: No known workaround. This is a display issue.
- A VLAN interface that is configured as a DHCP client may attempt to acquire an IP address even if the VLAN interface is shutdown.
  - Workaround: Remove the command ‘ip address dhcp’ from the vlan interface configuration.
- On NetVanta 123xPs, the switchport may begin flapping if “power inline” is disabled on a port where a legacy PoE device is plugged in.
  - Workaround: Unplug legacy PoE device first, then disable “power inline”.
- The command ‘ip igmp snooping vlan <vlan ID> mrouter’ may incorrectly be saved to the startup-config causing output errors on startup.
  - Workaround: Use ‘ip igmp snooping’ command without mrouter specified.
- The NetVanta 1534 and 1234 may fail to locate the IGMP router for transmitting IGMP requests even when the multicast router interface is known.
  - Workaround: Do not use IGMP snooping.
- Attempting to filter the Desktop-Auditing client list by IP address may result in an error stating “%Error: Invalid IP Address.”
  - Workaround: View client list without filtering.
- Enabling VRF forwarding on a PPP interface may cause the AOS device to reboot.
  - Workaround: Before enabling VRF forwarding, shut down the PPP interface and then apply it.

- Configuring stacking may cause the AOS device to reboot.
  - Workaround: Do not configure stacking.
- Using HDLC to do bridging with IRB may cause a reboot.
  - Workaround: Use PPP with bridging instead.
- ADSL Annex M will not train up when the training mode is set to multimode or Annex M.
  - Workaround: Downgrade firmware to 17.05.02.

## Resolved Issues

*These are issues that have been resolved since the previous AOS release (17.08.02)*

### Services and Viewers

- Enabling email-logging may cause the AOS device to reboot.
- When configuring the ATM sub-interface through the GUI, when setting the interface mode to PPPoE, the GUI will redirect a user to the ATM configuration page instead of the PPP configuration page.
- Receiving an invalid DHCP packet may cause a reboot.
- SNMP source interface may not source an SNMP packet from the specified IP address.
- The NetVanta 4305 may display an incorrect reset cause.
- The NetVanta 3430 may experience a clock drift that results in NTP frequency errors.
- The Security dashboard may incorrectly display the “Projected Average” of threat occurrences per day.
- An AOS device may lose the command to track a gigabit-Ethernet interface after a reboot.
- The telnet client may function improperly when being sourced from non-default VRFs.
- In the web GUI, the troubleshooting page may incorrectly display an error when GRE tunnels are configured stating, “Warning: tunnel 1 has a private IP address, but NAT is not enabled for its policy class.”
- The local-user list may be deleted from the running-configuration when TACACS+ is configured in a certain manner.
- If traffic traversing a NetVanta device is using gigabit-ethernet interfaces, a Netflow packet may mark the input and output interfaces as "0" instead of its correct IfIndex number.
- When downloading the configuration file from the web GUI, the AOS device may download the HTML script instead.
- In the GUI, adding a sub-interface on a NetVanta router with 802.1q encapsulation enabled may cause a lock up.
- When configuring Netflow export settings through the web GUI, an invalid warning is displayed in the CLI stating, “Warning: Interface not found. Source IP address will be set by routing.”
- When AAA is enabled, the FTP server may be unable to authenticate users via the default AAA list.
- Disabling DoS protection against threat ID 6 (TCP SYNs with a source port less than 1024) may not take effect until the NetVanta device is rebooted.
- Issuing the SNTP server 'source-interface' command may not properly source the SNTP packet from the specified interface's source IP address.
- An incorrect warning regarding a track may be outputted when an administrative distance is applied to a PPP interface set to 'ip address negotiate.'
- The mail-client may not send an email notification if there are no capture commands configured and the body of that email is empty.
- Certain mail-client configurations may cause improper bootup and instability that could result in the AOS device locking up.
- The output of 'show interface status' may show all unconnected ports as being connected at 100/full until the link status of the disconnected port is changed.
- SMTP messages originating from an AOS device may be rejected by some mail servers.
- The 'test if interface <interface>' command may be removed from the configuration after a reboot.
- The DNS service may strip the domain name from targets that are received from the DNS server when the query

to the first listed server times out.

- The packet count for the Top Traffic Statistics may be displayed incorrectly in the GUI.
- The output of the “show desktop-auditing dhcp brief” command may display false information.
- When using Microsoft Desktop Auditing, releasing and renewing the IP address on a client may not cause the NetVanta device to properly read the NAP information correctly from the new DHCP request.
- If a switchport of an AOS device is set to trunk mode, attempting to run the ‘Setup Wizard’ may cause it to hang on the ‘System Info’ page.
- Executing the ‘show desktop-auditing dhcp interface <interface>’ command, may return an error.
- Issuing the ‘show desktop-auditing dhcp’ command may show ‘Unknown’ for the ‘Client Automatic Updates’ state for a Vista NAP-enabled client.
- In the Web GUI, the ‘Port-Mirroring’ webpage will not allow the selection of a destination port.
- Enabling the URL filter may cause HTTP downloads to slow down or stall.

## **Routing, Switching and Bridging**

- The NetVanta 2<sup>nd</sup> Gen 1534 and 2<sup>nd</sup> Gen 1544 may reboot without an exception report or coredump message.
- An AOS device may reboot if an IGMP packet is received on a non-default VRF.
- Loopback interfaces may not be populated in the Layer 3 hardware table.
- The web GUI of the NetVanta 4430 may accept a gigabit-ethernet as a next-hop even though the option is invalid.
- On a 1544, ARP entries for multiple IP addresses that use the same MAC address may not properly be indexed for Layer 3 switching.
- Deleting a route on a NetVanta 1544 may cause any routing additions that occur afterwards to be software routed instead of being Layer 3 switched.
- Modifying a route-map that is used on an interface where FFE is enabled and is attempting to update may cause the NetVanta device to reboot.
- Configuring BVI interfaces for "ip unnumbered" before configuring the logical interfaces that will participate in the BVI interface may cause those logical interfaces to lose their configuration upon a reboot.
- ARP table entries may not properly be refreshed after half of their TTL has elapsed, potentially leading to a small number of dropped packets while the entry is being updated.
- A route-map name that contains a space may be lost when an AOS device is rebooted.
- Switchports that are part of a port-channel may remain in a suspended state after going down and then coming back up, causing traffic to be incorrectly directed through the port-channel.
- On a NetVanta 5305, if “ip ffe” is enabled on the PPP interface, issuing the command, ‘no ip address’, may cause a reboot.
- A hub connected to a NetVanta switch, may not be detected as a ‘shared link’ and may cause a packet storm to occur if there are multiple links between the switch network and the hub. This can eventually lead to a reboot of the NetVanta Switch.
- Stacking candidates may fail to create a Stack VLAN interface even when the Stack Master is known and the Stacking VLAN has been created.
- A topology change may cause the stacking VLAN interface to not come back up after going into a down state.

## **Network Interfaces and Quality of Service**

- An Ethernet interface with 802.1q encapsulation enabled may discard valid packets as giants.
- The AOS chassis may incorrectly recognize a Verizon 3G NIM as a Sprint 3G NIM when attempting to go through the activation process.
- The switchport interface statistics may show an incorrect and very high number of unicasts.
- Secondary IP addresses may be unable to be removed from Ethernet sub-interfaces.
- The cellular interface may be brought down due to short-term signal dropouts.
- The modem on a 3G NIM may not initialize if a T1 NIM is also installed.

- A PPPoE link may take an excessive amount of time (several hours) to come up.
- The output of a 'show qos map interface <interface>' may not report any packets matched, even though packets are being matched and prioritized appropriately.
- An Annex B ADSL link may not be able to train up properly.

## **Firewall and VPN**

- The output of 'show ip policy-sessions' may not display all active GRE sessions.
- Certain encrypted packets by the Shrew VPN client may be dropped when the packet is decrypted.
- Firewall event messages may be outputted even if the firewall is disabled.
- The 'ip rtp firewall-traversal' command is not retained after reboot.
- Policy timeout values for port 443 (HTTPS) may be lost after a reboot.
- When using the SIP ALG, under certain circumstances the public to private BYE may not be forwarded through the firewall causing the public side RTP passive session to not be created and not translating it by NAT to the correct public source port.



# AOS 17.09.02.00 Release Notes

Release Notes

Release Date: Dec. 7, 2010

Notes Revision: Dec. 7, 2010

## New Features

## Overview

### Strict Rate Policing

This AOS feature adds the ability to drop priority traffic that exceeds a specified limit, even when the egress interface is in a non-congested state.

**Supported Platforms** NetVanta 1335, NetVanta 3305, NetVanta 3430, NetVanta 3448, NetVanta 3450, NetVanta 3458, NetVanta 4305, NetVanta 4430, NetVanta 5305

## Resolved Issues

*These are issues that have been resolved since the previous AOS release (17.09.01)*

Issuing the command 'show tech' simultaneously from two separate sessions may cause the unit to lockup.

The NTP hardware and software clock on an AOS device may drift resulting in event messages stating, "NTP frequency error -500 PPM exceeds tolerance of 500 PPM."

When PPP fragmentation is enabled, fragments may traverse the same link instead of being transmitted equally between all the links.

Bridged frames across a PPP link with the "LAN FCS" bit set were given an extra CRC, which can cause an invalid packet to be transmitted and may result in errors.

A PPP interface may get stuck in loopback if the far end transmits LCP frames that do not include "magic numbers."

The DHCP server may incorrectly respond to a DHCP Request message from a client that it already gave an address to on a different interface.

On the 123x switches, if port security with sticky MAC addresses is used, the sticky MAC addresses may be removed after a certain period of time.

On a re-INVITE where both the remote IP and port number have changed, the SDP information is not properly processed by the SIP ALG, which may create an invalid policy session and result in one-way or no audio.

Mail clients configured to log or send email before a configuration has been fully loaded may cause the AOS device to lockup.

Issuing the command 'set metric 0' within a route-map may not be displayed in the running-configuration.



Issuing the 'debug atm oam <interface.sub-interface> loopback end-to-end' command with the incorrect syntax may cause a reboot.

When using Policy-based routing, setting an 'ip default next-hop' and having traffic match the default-route may cause a reboot.

When configuring 'match-all' QoS maps in the CLI, an invalid error message of, "%Cannot add multiple 'match dscp' statements to a map with 'match-all' enabled." may be displayed.

In the 123x switch GUI, the "Default Gateway" link may be missing.

Issuing the 'show mac address-table dynamic' command may cause a reboot.

Configuring a QoS map to match on an ACL that has a space in its name may disappear upon a reboot.

When 'service password-encryption' is enabled, a username or password configured for a PPP connection may display in clear text when it should be encrypted.

Policy-sessions created using an 'allow' policy-class entry may not be cleared when 'fast-nat-failover' is enabled.

A NetVanta 31xx device may not allow dial-in access through its modem interface.

When a large number of DHCP pools are configured, issuing the 'show run' command may cause the unit to become unresponsive for a period of time.

The Web GUI may display a switchport speed as "10 Mbps / full" even if it has been manually set to "2500 Mbps / full" in the CLI.

A QoS map that is matching a DLCI value may display an invalid error stating, "%Can only assign this QoS map to a frame relay interface." when applied to a frame-relay interface.